SharkStriker

Assisted a litigation firm in identifying weakenesses and boosting security posture

Outcomes Delivered

- Reduced time to detect threats by 75%
- Over 1k assets monitored across the United States
- Helped save 60% of costs due to non-compliance

SharkStriker Solutions

Managed SIEM & SOC Services

USE CASES

- 24x7 SOC
- Security testing (Pen-testing)
- SIEM management and monitoring

SharkStriker

Challenges

To eliminate alert fatigue and address critical alerts with context

As a litigation firm working with some of the largest companies in the world, they needed to ensure the confidentiality, privacy, and security of their clientele's case-related data.

They had a SIEM solution for continuously monitoring activities across the infrastructure and adherence to compliance requirements.

However, it became more challenging to manage the solution given the high volume of alerts with little context, color, or visibility. There was a challenge of a high number of false positives that not only cost the security team their time but also missed out on critical alerts to be addressed.

It was a challenge for them periodically to identify the security gaps in their security posture was a challenge due to lack of context. They were looking for round-the-clock expertise that could help them address all these challenges.

Ensuring the confidentiality, privacy, and security of client case-related and other data was critical to the firm's reputation.

- Their AlienVault SIEM overburdened their team with high false positives
- There was a major loss of time on security investigations due to lack of context
- They missed a majority of critical alerts that could pose a significant risk to their organization's security posture
- They had very little visibility of all the known and unknown vulnerabilities across their posture and loopholes that attackers could leverage to orchestrate a full-blown attack.

Civil Litigation Services

Our client was a highly reputable civil litigation law firm based in Carlsbad, California, with more than thirty years of working with a team of skilled attorneys. They have been representing some of the largest Fortune 500 Companies. They specialized in providing legal services specific to bankruptcy matters, replevin, and minimization of liability exposure.

Additionally, they also provided post-judgment recovery and compliance management services. Their focus is on maximizing legal recoveries for their clients by leveraging their expertise in civil litigation and judgment enforcement.

SharkStriker

Solution

The firm researched more than a hundred cybersecurity experts in the US. They were searching for a single-stop solution that could help them identify and address risks across their posture, ensure continuous monitoring of the security posture, and provide them the visibility and control of security operations. They found that among all the experts in the market, only SharkStriker was able to balance cybersecurity and compliance and address all their risks and challenges holistically.

"We were looking for a team of cybersecurity experts who can take over our cybersecurity operations while we focus on improving our service quality.

SharkStriker has helped us address all our cybersecurity and compliance challenges, from identifying all the security risks across the posture to helping us gain enhanced visibility of our security operations and make the most of our SIEM. They have made it all possible for us."

- Founder, CEO

False positives reduced by 96%

4000+
hours saved on response

Time to respond
1hr → 2 mins

SharkStriker

Results

Single-pane glass visibility of risks across posture.

SharkStriker integrated their open-architecture, multitenant platform STRIEGO, which was purpose-built to simplify cybersecurity.

Through automated periodical CIS-based assessments of posture, STRIEGO offered a comprehensive reportage of risks as per their severity. It helped the firm serve two goals (cybersecurity and compliance) with one. With multiple real-time dashboards, they were able to gain insights into their posture and make decisions with more context on the risks across the posture.

"Through SharkStriker's STRIEGO were able to gain better visibility of what was going on in cybersecurity. It gave us a single-stop view of operations along with insights on the posture that made sense to us. We were able to gain periodical reports to help us track the health of our security posture."

- Founder, CEO

Undisrupted security from threats.

With SharkStriker, the firm has a 24x7 team, rendering security 365 days a year, with dedicated expertise, providing them with the clock security they need to keep their operations and sensitive assets secure.

The team provided them with the dedicated expertise they needed, including security analysts, incident responders, threat hunters, threat researchers, domain experts, and DevSecOp engineers.

They provide the domain expertise needed for cybersecurity activities like analyzing incidents, identifying threats based on threat intel, determining the nature and techniques of attackers, and analyzing the best strategy for incident response and containment.

"Managing cybersecurity with the rising complexity and shortage in the workforce was a big challenge for us that SharkStriker helped us solve. They helped us bridge the gap and identify and implement best practices across our cybersecurity solutions through their platform STRIEGO".

- Founder, CEO

SharkStriker

Holistic fulfilment of GRC goals with SIEM.

The firm's SIEM solution was integrated with STRIEGO, which had an in-built SOAR that, with the help of AI and ML automatically responded to suspicious activities based on playbooks custom-crafted by security experts at SharkStriker. It helped them reduce the false positives by up to 96% and assisted the experts in focusing on critical alerts. They helped the firm make the most of their SIEM solution through actions like log management, identification and deployment of alert rules, compliance management, and automated response to threats.

"SharkStriker has helped us turbocharge our SIEM solution to the next level. They have assisted us in implementing industry best practices, providing us the centralized visibility control and instantaneous detection and response capabilities through their cutting-edge platform STRIEGO."

- Founder, CEO

80% reduction in time spent to investigate

95% reduction in fatigue due to events generated from customized playbooks

DISCOVER OTHER CASES BY US FROM A SPECIFIC INDUSTRY

CLICK HERE TO READ

Phone: +1 925 5321900
Email: sales@sharkstriker.com
Website: www.sharkstriker.com

Visit SharkStriker